

# **Индивидуальный проект Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование**

---

Кузьмин Артем

17 мая, 2025, Москва, Россия

Российский Университет Дружбы Народов

## Цели и задачи

---

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

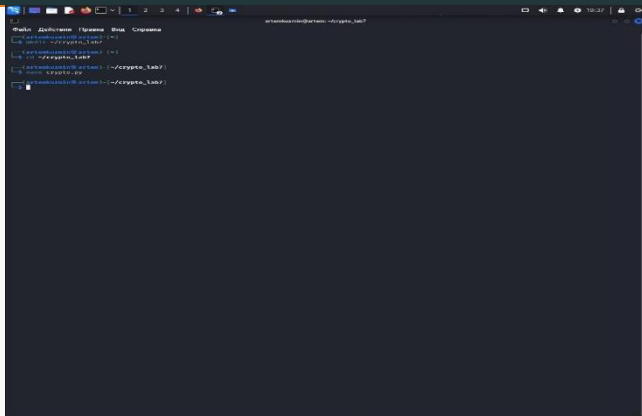
## Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования.

# **Выполнение лабораторной работы**

---

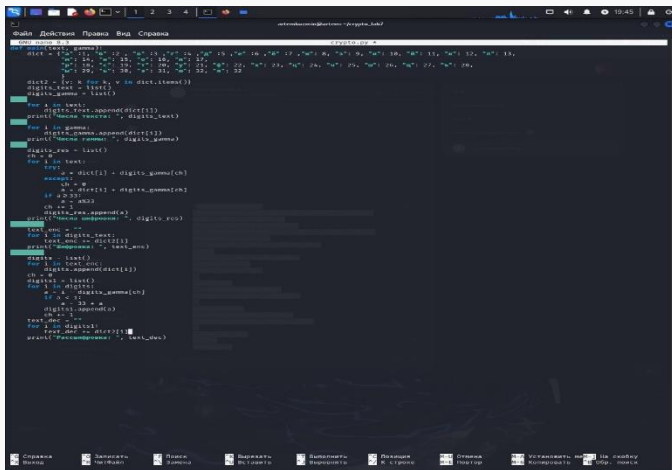
# Программа simpleid



```
artemkuznetsov@artem: ~/crypto_lab7
$ gcc simple.c -o simpleid
$ ./simpleid
simpleid: error: no input data
$
```

Рис. 1: Создаем исполняемый файл

## Программа simpleid2



### Рис. 2: Код файла

# Программа readfile

Длина текста: 19

Длина гаммы: 19

Текст: С Новым Годом, друзья!

Гамма: абвгдеёзийклмнопрс

Числа текста: [33, 0, 15, 16, 3, 13, 10, 0, 4, 16, 5, 16, 14, 12, 0, 5, 18, 21, 9, 33]

Числа гаммы: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19]

Числа шифровки: [32, 2, 12, 20, 6, 11, 13, 8, 13, 26, 14, 28, 3, 2, 15, 21, 7, 7, 50]

Расшифровка: С Новым Годом, друзья!

Шифровка: бвлтжкмимюоцвгпкк2

**Рис. 3:** Выходная информация



## **Выводы**

---

Изучили алгоритмы шифрования на  
основе гаммирования